ここでここでは、 金田士 こうしょい ひん かん ROJE PANICKAS 1/0×1/1/0×1/ 105 422res

.

(cotificate clain) #Hibukstr ENTY IL Signature Trusfellast Publiz Key PKIN PublizkeyA Cak Kat Calder a mandale Registration Authority Signature · (Certificate Chain) Public KeyA AHribuk Set 1 Trusted Rad 7 Cert. Lib. Addr. 106 Tother Data Certificate Library 202 105

r.hiji

Lertiticate Authority Registation Authority
X/Z Bank ~302 Caraholder Publishey 306 XYZBank Private Key XYZ Bank Public Key Certificate Library Reliant Party System)irectory 308 Card Interface Device INEMA ACCES PERCE Lungue identifier> CAS Secret Keys <u>3</u> 116,2

FIG. 4A **BEGIN** CREATE SECURE, AUTHENTICATED **CONNECTION BETWEEN IAD** 402 AND RELIANT PARTY IAD READS LDAP 404 ADDRESS FROM CHIP CARD IAD OFFERS ADDRESS TO 406 **RELIANT PARTY WHICH MAKES BIND ACCESS REQUEST RELIANT PARTY CREATES** 408 SECURE AUTHENTICATED CONNECTION TO CERT. LIBRARY **RELIANT PARTY CREATES AN** 410 **AUTHENTICATED SESSION WITH CERTIFICATE LIBRARY** RELIANT PARTY MAKES REQUEST 412 TO CERTIFICATE LIBRARY AND **GETS RESPONSE** Α

FIG. 4B



